Cybersecurity policy and its implementation in Indonesia

Rizal, Muhamad; Yani, Yanyan M.

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Cybersecurity Policy and Its Implementation in Indonesia

Muhamad Rizal *Universitas Padjadjaran, Indonesia*
Yanyan M. Yani *Universitas Padjadjaran, Indonesia*

Abstract

The purpose of state defense is to protect and to save the integrity of the Unitary State of the Republic of Indonesia, the sovereignty of the state, as well as its security from all kinds of threats, whether they are military or non-military ones. One of the non-military threats that potentially threatens the sovereignty and security of the nation-state is the misuse of technology and information in cyberspace. The threat of irresponsible cyber attacks can be initiated by both state and non-state actors. The actors may be an individual, a group of people, a faction, an organization, or even a country. Therefore, the government needs to anticipate cyber threats by formulating cyber security strategies and determining comprehensive steps to defend against cyber attacks; its types and the scale of counter-measures, as well as devising the rules of law.

Keywords: Cyber-attacks threats, cyber security strategies

Introduction

In the era of globalization, cyberspace has become a staple of human life, and it connects people regardless the distance. Cyberspace is a new world brought forward by the internet (Mahzar, 1999, p. 9). Paul Wagner (2010) argues that cyberspace is beyond every computer system that's connected by wire. Cyberspace also includes:

- isolated networks (private, corporate military);
- laptops and other personal PCs connected some of the time (wireless, modems);
- industrial control machinery, including programmable logic controllers (PLCs);
- industrial robots (connected to PLCs or directly to computers);
- home control equipment (home appliances and their control units);
- mobile devices (smartphones, PDAs); and
- USB and other storage devices.

Cyberspace displays reality, albeit not a tangible one. It is a virtual world, virtual reality, a world without borders. This is what is meant by the borderless world in a way that cyberspace does not recognize state borders, and it eliminates the dimension of space, time and place (Purbo, 2000, p. 50). It enables its citizens to connect with anyone anywhere as Bruce Sterling (1992) argues:

Journal of ASEAN Studies, Vol. 4, No. 1 (2016), pp. 61-78

ISSN 2338-1361 print / ISSN 2338-1353 electronic

> *Although it is not exactly "real," "cyberspace" is a genuine place. Things happen there that have very genuine consequences. This "place" is not "real," but it is serious, it is earnest. Tens of thousands of people have dedicated their lives to it, to the public service of public communication by wire and electronics.*

The concept of cybernation sparks the hope of bringing convenience, happiness, and endless opportunities to people. However, it comes with a price. Cyber security is a real and urgent necessity since its effects could potentially damage or disrupt people's lives, states, and even the whole world (Piliang, 1999, p. 14-15).

The urgency of cybersecurity is the more urgent because the internet has a particular darker side, e.g. it is widely considered to provide access almost exclusively to pornography. A recent well-publicized survey suggested that over 80% of the pictures on the internet were pornographic. While the survey result itself was found to be entirely erroneous, the observation that the internet can and does contain illicit, objectionable or downright illegal material is perfectly valid. It also supports fraudulent traders, terrorist information exchanges, pedophiles, software pirate, computer hackers and much more (Barrett, 1997, p. 21).

The world has long been concerned with cybercrime. In fact, one of the topics discussed at the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders in Vienna, Austria, 2000 was Crimes Related to Computer Network. However, not every state has cybercrime laws, and not all of them are considerably concerned about this issue (only developed countries and some developing countries are). This depends on how well-developed a state law is and how much it is concerned with the advancement of technology. This was revealed at the UN Congress in Vienna:

> *Reasons for the lack of attention to cyber crimes may include relatively low levels of participation in international electronic communication, low levels of law-enforcement experience and low estimations of the damage to society expected to occur from electronic crimes* (United Nations Office on Drugs and Crime, 2000).

As a developing country, Indonesia is a little left behind in keeping up with the development of information technology (Nur, 1998, p. 34), as a result of an improper strategy of technology development that ignores scientific and technology research. Consequently, the technology transfer from developed industrial countries is not followed by the mastery of the technology itself that turns Indonesia into a non-technological-based country. Alternatively, as Muhammad Nur (1998, p. 5-6) puts it, "Indonesia is a new pseudo-industrializing country."

Research Questions and Methodology

The fact that the Indonesia is still left behind in information technology raises the question of the condition of the implementation of cyber security policy in Indonesia. Therefore, this research seeks to discuss this problem.

The object of this research is cyber security in the context of law and national defense. The aspects of this discussion include law, national defense, and international relations perspectives. We will use realism theory as the analytical knife to see how Indonesia reacts to this international phenomenon. Realism is a school of thought that assumes that states compete for power. In International

Relations studies, power is one of the most used concepts (a mainstream concept) as well as the most controversial and hard to define (Perwita & Yani, 2006, p. 13).

In this article, the authors discuss the following questions:

1. How the cyber security policy and regulations implemented in Indonesia and what are the obstacles?
2. How is the implementation of cyber security-related policy and regulations in Indonesian in anticipating cyber attacks?
3. What steps should be taken by the government of Indonesia to anticipate cyber threats and attacks?

This research uses a multidisciplinary as well as interdisciplinary research design with a descriptive analytical method to describe the situation, condition, and all problems by using literature study to get a deeper understanding.

This article is structured into two parts: the first discusses the concepts related to cyber security, while the second analyzes the cyber security policy and its implementation in Indonesia. The first part talks about the shapes of cyber threats and attacks, then argues about the role of cyber security in national security. The second part discusses cyber security governance, related legislations and regulations, current policy, and related obstacles in Indonesia, then analyzes the development of cyber defense, the implementation of cyber security regulations, and three steps to strengthen cyber security in Indonesia.

The Shapes of Cyber Threats and Attacks

On 6 September 2007, Syria's nuclear power development facility was bombarded by Israel's aircraft. One of the issues that became the news was Syria's inability to prevent or operate its armed forces against such attack. There were many opinions and analysis on this. One of them said that it was because Israel had "disarmed" Syria's radar and military force by using information technology. In other words, Syria experienced a cyber attack (Clarke & Knake, 2010, p. 5).

The significant development of information technology has changed the world's face and shifted our understanding on what's understood as a nation's power, as well as showing us a diffusion of that understanding (Nye Jr, 2011, p. 1). A nation's power is neither just about how big the economy is nor how strong the military is, but it is also about the values it offers to the world, and one of them is its mastery of technology. In the 21st century, almost all activities, from personal ones to official ones, rely on the use of information technology. Israel's attack on Syria was one of the examples of the advanced use of information technology to support military activities.

The use of information technology for destructive purposes is a threat to a country's national defense. The threats can either be military or non-military ones. Military threats to national defense are threats to defense and security, while non-military threats to national defense are threats to the ideological, political, economic, social, and cultural resilience of a country. Sooner or later, the advance of technology will affect our cultural convention, socio-cultural institutions and (from socio-political perspective) our

government's decision-making patterns (Sudarsono, 1992, p. 4). Legal scholar Ari Purwadi (1993, p. 234) confirms this when saying that he believes technology represents a certain value system because it is a product of people's socio-culture.

In general, the elements that can be identified as potential sources of threats consist of internal and external sources, intelligence activities, disruption, investigation, extremist organizations, hacktivists, organized crime groups, rivalry, hostility and conflicts, as well as technology (The Ministry of Defense of the Republic of Indonesia, 2013, p. 24). Almost every country believes that science and technology are two important factors in supporting the growth and progress of a country. In the context of economic development, technology can act as an engine of economic growth (Frame, 1983, p. 7). Countries that do not have and master science and technology will be left behind. Science and technology are now glorified and have become an ideology. Some people worship technology so much and treat it as if it was the only way to welfare, prosperity, and justice.

In addition, a developed technology has created a new cult, a consumer society (Jacob, 1993, p. 13). Therefore, the use of information technology and the internet as a way to fight in cyber warfare, which threatens national defense and security, has become a common thing. In addition to being one of the aspects that endanger national security, there is an urgency to understand the aspects of legal regulations, particularly in the context of cyber law.

Cybercrime is a cross-border crime. Since it crosses borders and involves many countries, cybercrime is considered as an extraordinary crime. Thus, it is important to have multilateral agreements to tackle it, both in regional and international levels. The use of military force should be the last option. This is because a state cannot simply use a military force to carry out an attack or to start a battle. There are a lot of things to consider such as costs and budgets. The state should build a digital-technology-based cyber defense soon.

Some of the common forms of cyber threats today are as follow (The Ministry of Defense of the Republic of Indonesia, 2013, p. 25):

1. Advanced persistent threats (APT), denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks are usually done by overloading a system capacity and preventing legitimate users to access and use the targeted system or resources. These attacks are dangerous threats to organizations that rely almost entirely on the Internet's ability to run their activities;

2. Defacement attacks are carried out by replacing a victim's web page with a forged one, where the type of the contents depends on the criminal's motives (can be either pornography or politics);

3. Malware attacks are malicious programs or codes that can be used to disrupt the normal operation of a computer system. Usually, a malware program is designed to get financial profits or other benefits;

4. Cyber infiltrations can attack a system through the identification

of legitimate users and connection parameters such as passwords. These attacks are done by exploiting vulnerabilities that exist in the system. The main methods used to get access to the system are:

1) Guessing very obvious passwords, such as one's user name, the name of one's spouse or child, a date of birth or things which are important and related to someone or his family, so it is easy to guess and find out;

2) Exploiting unprotected accounts. Users can also make mistakes, by not entering a password or giving their password to others;

3) Fraud and social engineering. For example, the offender may claim and act as an administrator and ask for the password for some technical reasons;

4) Listening to data communication traffic. A tapper will listen to unencrypted data transmitted over the network via a communication protocol;

5) Trojan Horse, a specific spy program and a highly dangerous spyware. It can secretly record parameters used to connect to a remote system.

6) Exploiting the authentication system. All users' passwords should be stored on a server. A hacker will access the file that stores all users' encrypted passwords and then open it with tools available on the network;

7) Testing all the possible permutations that can be the key to cracking passwords, if a cracker knows cipher algorithm;

8) Spying. This is done by recording their connection parameters using software, spyware or multimedia devices, such as video cameras and microphones, to capture confidential information, such as passwords to access a protected system;

5. Spamming and Phishing. Spamming is the sending of undesired mass emails to:

1) Get publicity or for commercial purposes;

2) Introduce malicious software, such as malware and firmware into a system;

3) In the worst case scenario, spam may resemble a bomb attack, with the results of overloaded mail servers, full users' mailboxes and it could create a great discomfort in the email management. In the past, spam was only

considered as a nuisance, but today, spam is a real threat. It has become a special vector for the spread of viruses, worms, Trojan Horses, spyware, and phishing attempts;

6. Abuse of Communication Protocol. A spoofing attack of Transmission Control Protocol (TCP) relies on the fact that the TCP establishes a logical connection between systems to support the exchange of data. This allows it to get through a firewall and establish a secure connection between two entities, a hacker, and a target.

In addition to the above cyber threats, there are other types of cyber attacks. These cyber attacks can be categorized into (Carr, 2009):

1. Hardware threats. These threats are caused by the installation of certain equipment that serves to perform certain activities in a system. Therefore, the equipment is a disruption to the network system and other hardware. For example, jamming and network intrusion;

2. Software threats. These threats are caused by the software of which functions are to steal information, to destruct information/system, to manipulate information (*Information Corruption*) in a system, and others.

3. Data/information threats. These threats are caused by the spread of certain data/information for a certain motive. What is done in information warfare is considered propaganda.

Cyber Security Role in National Security

A weak cyber defense may create tensions among countries and disrupt the stability of security, create social, economic, and environmental impacts, as well as disrupt the relationship among countries (Ghernaouti-Hélie, 2009, p. 24).

Cyber security has two key words: cyber and security. Talking about cyber means talking about information, connections (telecommunications, networks), gateways (computers, devices, users), rooms, or spaces, and it is about involving, using, or relating to computers, networks, and the internet. Meanwhile, security is usually related to assets and assets protection. Security is protecting the asset, protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction, protecting information and systems from major cyber threats (Ghernaouti-Hélie, 2009, p. 28).

Computer security, cyber security, or IT security is information security applied to a computer or a network. Computer security aims to help users prevent fraud or detect any attempts of fraud in an information-based system. The information itself is non-physical.

Cyber security is an effort to protect information from cyber attacks. Cyber attacks in information operation mean all deliberate actions to disrupt the confidentiality, integrity, and availability of information. This action can be in a form of physical disruption or a disruption of the logical flow of information system. A cyber attack is an attempt to disrupt information which focuses on the logical flow of information system. National Cyber Security is a term used for cyber security that is related to the assets/resources of a country (Boisot,

1998, p. 18). The objective of national cyber security is the protection, domination, and control of data and information. National cyber security is closely related to information operation, which involves various parties such as the military, the government, state-owned enterprises, academia, private sectors, individuals, and the international world. The continuity of information operation does not only rely on cyber security itself, it also depends on physical security, which is related to all physical elements such as data center buildings, disaster recovery system, and transmission media.

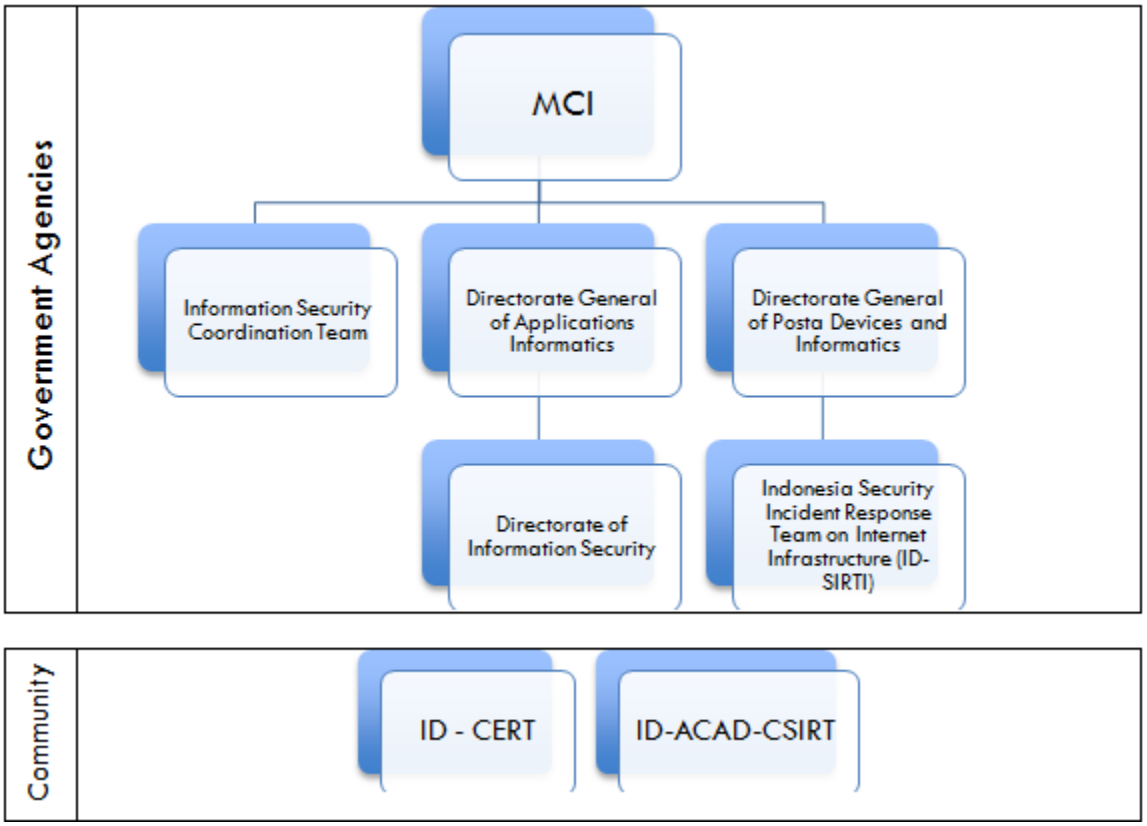
Cyber Security Governance in Indonesia

In terms of cyber security, Indonesia already has a system and strategy of cyber security conducted by government agencies and also the official community. Cyber security policy is coordinated by the Ministry of Communication and Informatics (MCI). There are three government organizations involved in cyber security in Indonesia, which are Information Security Coordination Team, Directorate of Information Security, and Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII).

The Information Security Coordination Team was formed in April 2010 to coordinate cyber security, focusing on the expertise and the practice in the field of information and technology. The Directorate of Information Security has the tasks of policy formulation and implementation, training, monitoring, evaluation and reporting in the field of information security governance. Lastly, ID-SIRTII was established by the government based on Regulation of the Minister of Communication and Informatics No. 8 of 2012 to handle security on internet infrastructure.

Meanwhile, there are two community organizations involved in cyber security in Indonesia. Acting as a supporting institution, Indonesia Communication Emergency Response Team (ID-CERT) is an organization that works with the government in special cases to support the development of cyber security in Indonesia. In addition, ID-CERT also functions as a supporting institution for government organizations (Setiadi, Sucahyo, & Hasibuan, 2012, p. 111) such as the ID-SIRTII. Another community organization is the Indonesia Academic Computer Security Incident Response Team (ID-ACAD-CSIRT), the organization for the universities that want to focus on the development of security in Indonesia. ID-ACAD-CSIRT currently has 40 members of academic CSIRT universities.

Figure 1. Organizational Structure of Cyber Security Governance in Indonesia



Source: Setiadi, Sucahyo, & Hasibuan (2012), p. 111

Cyber Security-Related Legislations and Regulations in Indonesia

The government of Indonesia has created a policy concerning the implementation of cyber security in its legislation based on the Law No. 11 of 2008 on Electronic Information and Transaction (ITE). There are several other laws that are indirectly related to the policy, but related to such information, such as the Law No. 36 of 1999 on Telecommunication, and the Law No. 14 of 2008 on the Openness of Public Information.

In addition, the following are the laws supporting the implementation of cyber security:

1. Law No. 8 of 1999 on Consumer Protection,
2. Law No. 2 of 2002 on State Police of the Republic of Indonesia,
3. Law No. 3 of 2002 on State Defense,
4. Law No. 15 of 2003 on the Enactment of Government Regulation in Lieu of Law No. 1 of 2002 on Terrorism and Crime Eradication as a Law,
5. Law No. 34 of 2004, on Indonesian National Armed Forces, and
6. Law No. 25 of 2009 on Public Service.

Up to now, the government regulation as law enforcement, which supports the implementation of national information security policy, is still being processed by the MCI. However, some presidential regulations have become a reference in the implementation of national information security policy. Some of the regulations are:

1. Presidential Instruction No. 3 of 2003 on the National Policy on E-Government Development,
2. Presidential Regulation No. 20 of 2006 on National Board of Information and Communication Technology (ICT), and
3. Presidential Regulation No. 41 of 2010 on General Policy on State Defense Year 2010–2014.

Meanwhile, the MCI as the ICT regulator has released some regulations as implementation guidelines, such as:

1. The Regulation of the Minister of Communication and Informatics No. 29 of 2006 on the Certification Authority Implementation Guidelines,
2. The Regulation of the Minister of Communication and Informatics No. 28 of 2006 on the Use of go.id Domain Name for All Central and Local Government's Official Websites,
3. The Regulation of the Minister of Communication and Informatics No. 30 of 2006 on the Watchdog Committee of Certification Authority,
4. The Regulation of the Minister of Communication and Informatics No. 41 of 2007 on the General Guidelines of National ICT Governance,
5. Ministerial Decree of the Minister of Communication and Informatics No. 57 of 2003 on the Guidelines to the Making of Institution's E-Government Development Master Plan.

To optimize the implementation efforts, the issued regulations require additional materials and elaborations on implementation strategies, cooperation model, and organization. In addition, implementing national cyber defense needs cross-institutional coordination (The Ministry of Defense of the Republic of Indonesia, 2013, p. 35).

Current Cyber Security Policy in Indonesia

Indonesian cyber security policy was initiated back in 2007, following the release of the Regulation of the Minister of Communication and Informatics No. 26/PER/M.Kominfo/5/2007 on the Security of the Use of Internet-Protocol-Based Telecommunication Network, which was later replaced by the Regulation of the Minister of Communication and Informatics No. 16/PER/M.Kominfo/10/2010. This was then updated with the Regulation of the Minister of Communication and Informatics No. 29/PER/M.Kominfo/12/2010. An important aspect in the regulation is the establishment of ID-SIRTII. The Minister of Communication and Informatics assigned the team to help control the security of Internet-protocol-based telecommunication network.

ID-SIRTII's functions and tasks are to watch and to detect early and warn when any disruptions on the network

occur. The team also coordinates with related parties at home and abroad when it needs to secure the network. The team also provides information when threats and disruptions come up. Finally, ID-SIRTII also works on devising work plans (Article 9 of the Regulation of the Minister of Communication and Informatics No. No.29/PER/M.Kominfo/12/2010).

According to Hasyim Gautama, the framework of cyber security law in Indonesia was based on Law No. 11 of 2008 on Electronic Information and Transaction, Government Regulation No. 82 of 2012 on the Implementation of Electronic System and Transactions, as well as ministerial circulation letters and minister regulations (Ardiyanti, 2014).

Aside from the initiation of cyber security-related legislations, to ensure legal certainty in the development of cyber security, the government enacts the cyber security national framework. However, the legal framework for cybercrime-handling is still weak. Despite the existence of the law that forbids any forms of attacks or vitiation to the electronic system, no law that specifically regulates and contains cybercrime is available. Meanwhile, cybercrime evolves and takes place rapidly, making it hard for the law enforcers to handle it.

The Cyber Security-Related Obstacles to Deal with

According to Hasyim Gautama, there are several obstacles that we have to deal with concerning cyber security development on a national scale, such as (Ardiyanti, 2014):

1. State administrators that have weak understanding of cyber security issues,
2. Some internet services that have servers located abroad,
3. Lack of a secure system in Indonesia,
4. The absence of law that specifically addresses and regulates attacks in cyber world,
5. The frequent happenings of cyber crime that render it hard to handle,
6. The issues with the governance of national cyber security institutions,
7. Weak awareness of international threats of cyber attacks that can paralyze a state's vital infrastructures, and
8. Lack of industries that produce and develop IT-related hardware to strengthen our defense in the cyber world.

The handling of cybercrime is partial and its nature tends to be scattered due to the absence of a standard coordination. It is substantially dangerous because cyber attacks can paralyze a state's vital infrastructures. For example, Soekarno-Hatta International Airport's radar system has been disrupted a couple of times. It is always possible that cyber attacks do such things to a country's vital infrastructure.

Indonesia needs a policy that regulates all elements related to cyber security. In all policies that regulate ICT system, the communication used includes all regulations that need a standard document as a reference to run all information-security-related processes. This infrastructure standard has to meet the international standard to face a cyber war. It needs to have proper perimeter defense and a network monitoring system.

In addition, the policy governing the ICT system requires an information system and event management which can monitor security incidents on the network. It also needs network security assessment that controls and measures security.

The Development of Cyber Defense in Indonesia

The Law No. 3 of 2002 on State Defense states that the purpose of state defense is to protect and save the sovereignty and territorial integrity of the Republic of Indonesia and the safety of the nation from all kinds of threats, whether military or non-military ones. Indonesia needs to improve its soft and smart power in defense to anticipate cyber war through deterrence strategy as well as through the prosecution and recovery of cyber defense. This will support cyber security national strategy as promoted by the MCI (Ardiyanti, 2014, p. 1).

Law No. 11 of 2008 on Electronic Information and Transaction states that the use of information technology has to be secure in order to keep the confidentiality, integrity, and availability of the information. In that law, electronic information is legally acknowledged and any related actions are done by a law enforcer or a user has a legal responsibility (Ardiyanti, 2014, p. 1).

The above two laws give a mandate to government agencies, including to the Ministry of Defense (MoD), to take necessary steps to protect the sovereignty and territorial integrity of Republic of Indonesia and the safety of the nation, as well as the safety of cyberspace, where the electronic system works and benefits people.

Along with the MoD, The MCI as the leading government agency in telecommunication and informatics has five cyber security policy agendas in developing a secure cyber environment. They are doing it by implementing *"Ends-Ways-Means"* strategy model, which focuses on targets, priorities, and measured actions. The five policies are (Ardiyanti, 2014, p. 2):

1. capacity building,
2. policy and legal framework,
3. organizational structure,
4. technical and operational measures, and
5. international cooperation.

The ministry functions as the national information security regulator and the policies implemented will become a reference in formulating the national strategy's road map of cyber security.

In dealing with national interests, the MoD needs to understand, study, measure, anticipate and prepare actions needed to deal with things happen in the cyber world, which might come as threats to the state defense. Technology has transformed the shape of threats, from a conventional one to a virtual and asymmetrical one. These virtual threats exist, and their impacts are real. The threats might be small, ignorant of the existing law, coming from inside and outside the country with different modes and motives; yet, it can be destructive. This is why the minority can defeat the majority (Ardiyanti, 2014, p. 2).

In this globalization era, the implementation of public service highly depends on the availability, integrity, and confidentiality of information in cyberspace. In order to ensure a safe cyberspace for the sake of national

security, we need to realize that attacks in cyberspace may directly affect our state defense. Therefore, there should be a agreement that security in cyberspace is not just some computer security technical issues. In fact, it covers ideological, political, economic, social and cultural aspects as well as national security (Ardiyanti, 2014, p. 2).

Security issues in cyberspace are also national policy issues. Attacks in cyberspace may interfere with people's lives and national interests, such as economy, infrastructures, public health, national security, and safety, as well as state defense. The state needs to create a secure condition in cyberspace in order to ensure that Indonesian citizens and their homeland have a good social life, economy, state order, and protection. This agenda will be one of the main references in formulating cyber policies.

The utilization and mastery of technology, including information technology, shall accelerate, simplify, and ensure the solving of the state's strategic problems, not the other way around. Thus, the cyber defense cannot be done sporadically and on a case-by-case basis. It needs to be systematic, coordinated, and integrated.

Up to this day, the implementation of cyber defense in Indonesia has not been a coordinated national initiative. The implementation steps are still sectoral, and it highly relies on each of the sectors' interests and capability. The capability, deterrence, and countermeasures of cyber defense are very weak and vulnerable to massive attacks.

There have been some initiatives by some institutions and business entities in implementing cyber defense, such as (Ardiyanti, 2014, p. 36):

1. Government agencies/institutions:
    1) The MCI established ID-SIRTII in 2007,
    2) The National Cipher Agency (Lemsaneg) has a unit specialized in the security of ICT resources, especially those related to signals intelligence,
    3) The State Intelligence Agency and the Strategic Intelligence Agency also have special units on the security of ICT resources which are related to signals intelligence,
    4) The MoD and the Indonesian National Armed Forces have the initiative to build their internal cyber defense forces, run by the MoD's Center for Data and Information (Pusdatin), the Armed Forces' Center for Information and Data Processing (Pusinfolahta), and the service branches' Offices for Information and Data Processing (Disinfolahta), which are continuously being developed;
2. Education institutions and communities:
    1) An Indonesian ICT community, which worked with Communication Emergency Response Teams (CERTs) in some universities, established the ID-CERT,

2) Institut Teknologi Bandung, Universitas Indonesia, Universitas Gajah Mada, and Institut Teknologi Surabaya have started building and applying ICT security in their academic environment;

3. Business entities:

1) The telecommunication industry, pioneered by PT Telekomunikasi Indonesia (Telkom) as the owner and regulator of information and communication infrastructure, has set the standard to secure information and communication networks, which would then be applied to meet ISO 27001 standards,

2) The banking industry, under the guidance of Bank Indonesia, has implemented a security system on banking information infrastructure by following the guidelines of Bank Indonesia Regulation and international ICT security standards,

3) The gas and petroleum industry has also implemented the ICT security standards in each of their fields.

The role of inter-institutional coordination, to implement a national cyber defense, has not been done optimally by relevant agencies. The MCI has just started coordinating the security of information resources through ID-SIRTI.

In addition to domestic anticipation, the role of international cooperation is indispensable in order to support a successful implementation of cyber defense. To date, the role of international cooperation is still carried out sectorally by agencies, communities, and entities, in accordance with their own interests. They do this by joining international associations and parents of organizational institutions.

One of Indonesia's strategic alliances in cyber security policy is by cooperating with Association of Southeast Asian Nations (ASEAN) to deal with cyber security. It is one of Indonesia's commitments to realize ASEAN's three pillars, namely the ASEAN Economic Community, the ASEAN Socio-Cultural Community, and the ASEAN Political-Security Community. Another commitment is to have a stronger cooperation with ARF to support the three pillars. Indonesia was also one of the countries that initiated the Treaty of Amity and Cooperation (TAC). Substantially, the fellow member states do not attack each other and resolve conflicts in a peaceful manner (The Department of Defense of the Republic of Indonesia, 2008, p. 6, 42, 58).

Indonesia has also been consistently partnering with ASEAN in cyber security sector, because of the prominence of Malaysia's and Singapore's cyber security development. Malaysia has prepared cyber security supporting policies, institutions, infrastructures, and programs and the effort has been discussed in international cooperation forums. The institution in-charge that runs cyber security functions in Malaysia

is called Siberoc, which coordinates with Malaysia's information security institutions such as Malaysian Computer Emergency Response Team (MyCERT). Meanwhile, Singapore excels in its human resources, having the highest number of information security experts in ASEAN (The Ministry of Defense of the Republic of Indonesia, 2013, p. 17).

Indonesia and ASEAN have been consistently partnering in security sector because ASEAN has given some contribution to Indonesia to deal with cyber threats. In ASEAN Regional Forum (ARF), Indonesia and ASEAN work together in tackling cybercrime by improving security level in states' cyber sector.

Indonesia has been doing its part in cyber security by establishing bilateral and multilateral cooperation in international regional organizations, such as ASEAN. In 2006, the ARF focused on cybercrime threats and the meeting's theme was "Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space". A workshop on this was held during a meeting in Vietnam in 2012 (ASEAN Secretariat, 2013).

Previously, in a conference held in Kuala Lumpur, Malaysia, on January 13th-14th, 2011, the attendants agreed to form a community to improve cyber security in South East Asia region. As a result, ASEAN-CERT was established. In a conference in Mactan Cebu, Philippines, on November 15th-16th, 2012, they all agreed to continue the development of CERT and to support its tasks (ASEAN Secretariat, 2013).

Consequently, along with other ASEAN countries, Indonesia was committed to develop its cyber security and would consistently do so until the beginning of ASEAN Community in 2015.

The Implementation of Cyber Security Regulations in Indonesia

The way cyber security is handled in the framework of state defense is still sectoral, not well-coordinated nor integrated yet. As the MoD general secretary Eris Herryanto (2011) explained, the cyber defense concept that was implemented by the MoD and the Indonesian National Armed Forces is still sectoral, not comprehensive as a unity (Herryanto, 2012).

Therefore, the MoD established a cyber defense operation center team to tackle cyber crime as well as to secure and to protect the nation in the cyber world. The establishment of Cyber Defense Operation Center in the national cyber security policy is intended to build a universal defense system, which involved all citizens, territory, and other national resources, and to uphold the state's sovereignty, as well as to protect the territory integrity and the security of the entire nation from cyber threats.

One of the alternative policies is to put cyber security in defense context. Some policies that have been implemented are in defense context, as well. The Cyber Defense Operation Center, as has been explained above, is one of them. The Center has a working team established in 2010 that composed a plan to form an information security incident management team.

Three Steps to Strengthen Cyber Security

In order to strengthen cyber security, the Indonesian government shall adopt the following three steps:

1. Capacity building

Training programs and courses to upgrade cybersecurity skills should be conducted in coordination with Defense Cyber Operations Centre. Training for human resources on the importance of cyber security should be held to improve the understanding of preventive measures to prevent any acts of cybercrime.

In order to develop human resources' skills to deal with cyber security, the Indonesian National Armed Forces has conducted cooperation with some stakeholders who are highly skilled in information technology field. One of the stakeholders is Institut Teknologi Del (IT Del), North Sumatera. This cooperation was planned to last for three years, from 2014 to 2017, with three programs: the preparation of cyber warfare model, seminars on military cyber intelligence and cyber operations, and cyber camp or cyber weekend (JPNN.com, 2014).

2. International cooperation

The next step is to do international cooperation with regional and international organizations in order to tackle cybercrime. Indonesia has conducted cooperation to tackle cybercrime by becoming a member of ASEAN Network Security Action Council and International Telecommunication Union (ITU), becoming the steering committee of Asia Pacific Computer Emergency Response and Security (APCERT), and doing bilateral cooperation in the cyber security field with Japan, United Kingdom, and other countries.

Indonesia also plays an active role in Global Cybersecurity Agenda (GSA), which was launched in the 2007 World Telecommunication and Information Society Day. The GSA is an international cooperation of which main goal is to create a strategy and a solution to boost trust and improve security in the information society (Broto, 2008).

3. Legal certainty

In a legal context, cyber security development means the availability of security policy document as the standard document people refer to when running the whole information-security-related processes.

The development and the strengthening of cyber security policy in Indonesia should be integrated with a national strategy to build a national cyber security ecosystem, which has been prepared by the government. The national strategy includes legal efforts and technical efforts, such as operational standards of organization structuring, cyber security management institutes, human resource capacity building and the effort to improve international cooperation.

Conclusion

Indonesia has already had some policies that regulate cyber security; however, the nature of such policies is general (lex generalis, and therefore not specific (lex specialis). As a result, the implementation of cyber security has not been effective. In order to make them effective, the government needs to make them specific and, along with all of the stakeholders, continuously socialize them. In addition, the government needs to take the implementation of cyber security more seriously to anticipate cyber attacks. Singapore and Malaysia, among ASEAN members, have already had specific cyber

security policies, and this is in accordance with potential threats.

Indonesia, on the other hand, does not have a special institution with full authority to manage and deal with cyber security, yet. However, even without a special institution, the government should still be able to assign one of its structures or institutions to become a leading sector. This shows us that the implementation of cyber security is dispersed and that the government's role in the cyber defense is minor.

There are individuals who try to break the norms and the laws, violate rules and regulations, or take control over information security as well as physical assets in order to get material or non-material benefits. Therefore, the government needs to make some serious efforts to anticipate cyber threats and attacks and save Indonesian cyber defense from being a target of irresponsible parties.

About the Author

Muhammad Rizal is a Senior Lecturer at the Department of Business Administration, Universitas Padjadjaran. One of his research interests is on cyber security law.

Yanyan Mochamad Yani is a Professor in International Relations of Universitas Padjadjaran. His expertise is in international security studies especially non-traditional threat.

Reference

Books

Barrett, N. (1997). *Digital Crime: Policing the Cybernation.* London: Kogan Page Ltd.

Boisot, M. H. (1998). *Knowledge Assets: Securing Competitive Advantage in the Information Economy.* Oxford: OUP Oxford.

Carr, J. (2009). *Inside Cyber Warfare: Mapping the Cyber Underworld.* California: O'Reilly Media.

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It* (1st Edition ed.). New York: Harper Collins Publishers.

Frame, J. D. (1983). *International Business and Global Technology.* Maryland: Lexington Books.

Ghernaouti-Hélie, S. (2009). *Cybersecurity Guide for Developing Countries* (Enlarged Edition ed.). Geneva: International Telecommunication Union.

Jacob, T. (1993). *Manusia, Ilmu dan Teknolog.* Yogyakarta: PT Tiara Wacana.

Mahzar, A. (1999). Introduction. In J. Zaleski, *Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia (Trans.)* (p. 9). Bandung: Mizan.

Nye Jr, J. S. (2011). Cyber Power. In J. S. Nye Jr, *The Future of Power in the 21st Century* (pp. 1-24). Cambridge: Public Affairs Press.

Perwita, A. A., & Yani, Y. M. (2006). *Pengantar Ilmu Hubungan Internasional.* Bandung: PT Remaja Rosdakarya.

Piliang, Y. A. (1999). Introduction. In M. Slouka, *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan* (pp. 14-15). Bandung: Mizan.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books.

Sudarsono, J. (1992). *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial Politik.* Jakarta: Masyarakat Jurnal Sosiologi, FISIP UI-Gramedia.

Journals

Ardiyanti, H. (2014). Cybersecurity dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica , 5* (1), 1-26.

Nur, M. (1998, August). Dilema Pengembangan Infrastruktur Informasi Indonesia. *Info Komputer Vol. XII No. 8* , p. 34.

Purwadi, A. (1993). Kebutuhan Akan Perangkat Hukum Perjanjian di Bidang Alih Teknologi. *Hukum dan Pembangunan* (3 Th XXIII).

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012). An Overview of the Development Indonesia National Cyber Security. *International Journal of Technology & Computer Science (IJTCS) , 6* (November / December), 106-114.

Others

ASEAN Secretariat. (2013). ASEAN's Cooperation on Cybersecurity and against Cybercrime. *Octopus Conference: Cooperation Against Cybercrime* (pp. 1-20). Strasbourg, France: Council of Europe.

Broto, G. S. (2008, November 16). *Menteri Kominfo Pada "High-Level Segment ITU Council 2008" Yang Membahas Cybersecurity*. Retrieved from Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika: http://www.postel.go.id/info_view_c_26_p_814.htm

Defence Media Center/PPID. (2012, November 27). *Kemhan dan TNI Membangun Kekuatan Pertahanan Cyber*. Retrieved June 2, 2014, from Defence Media Center/PPID: http://dmc.kemhan.go.id/post-kemhan-dan-tni-membangun-kekuatan-pertahanan-cyber.html

Herryanto, E. (2012, November 27). Keynote Speech. *Seminar Nasional Keamanan Infrastruktur Internet tentang Trend Ancaman Infrastruktur Internet 2012* . Bandung, West Java, Indonesia.

JPNN.com. (2014, May 13). *TNI Gandeng IT Del Antisipasi Penjahat di Dunia Internet*. Retrieved June 2, 2016, from JPNN.com: http://www.jpnn.com/read/2014/05/13/234115/TNI-Gandeng-IT-Del-Antisipasi-Penjahat-di-Dunia-internet

Purbo, O. W. (2000, June 28). Perkembangan Teknologi Informasi dan Internet di Indonesia. *Kompas* , p. 50.

The Department of Defense of the Republic of Indonesia. (2008). *Indonesian Defense White Paper.* Jakarta: The Department of

Defense of the Republic of Indonesia.

The Ministry of Defense of the Republic of Indonesia. (2013). *A Road Map to Cyber Defense National Strategy.* Jakarta: The Ministry of Defense of the Republic of Indonesia.

The Ministry of Defense of the Republic of Indonesia. (2013). *A Road Map to Cyber Defense National Strategy.* Jakarta: The Ministry of Defense of the Republic of Indonesia.

United Nations Office on Drugs and Crime. (2000, April 10). *Crimes Related to Computer Networks - Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* Retrieved from United Nations Office on Drugs and Crime: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf

Wagner, P. (2010). *Computer Security and Cyberwarfare.* Retrieved from Department of Computer Science, University of Wisconsin-Eau Claire: www.cs.uwec.edu/~wagnerpj/talks/cyberwar.ppt